

Курс «Базы данных»

Тема. Объектные привилегии

Барабанщиков  
Игорь Витальевич

# План лекции

- **Объектные привилегии**
- **Предоставление и отмена объектных привилегий**
- **Проверка доступных привилегий**

# Объектные привилегии

- Объектная привилегия, выданная пользователю, позволяет ему **выполнять конкретные действия над определенным объектом (например, таблицей)**.
- Без специального разрешения пользователи имеют доступ только к своим собственным объектам.
- **Объектные привилегии выдаются владельцем объекта, либо пользователем, которому явно предоставлено право выдавать привилегии на объект.**

# Объектные привилегии Oracle

- **ALL** – все действия с объектом
- **ALTER** – изменение определения объекта
- **DELETE** – удаление строк из таблицы
- **EXECUTE** – выполнение хранимой процедуры
- **INSERT** – вставка строк в таблицу
- **REFERENCES** – создание ограничений
- **SELECT** – выборка строк из таблицы
- **UPDATE** – изменение строк в таблице

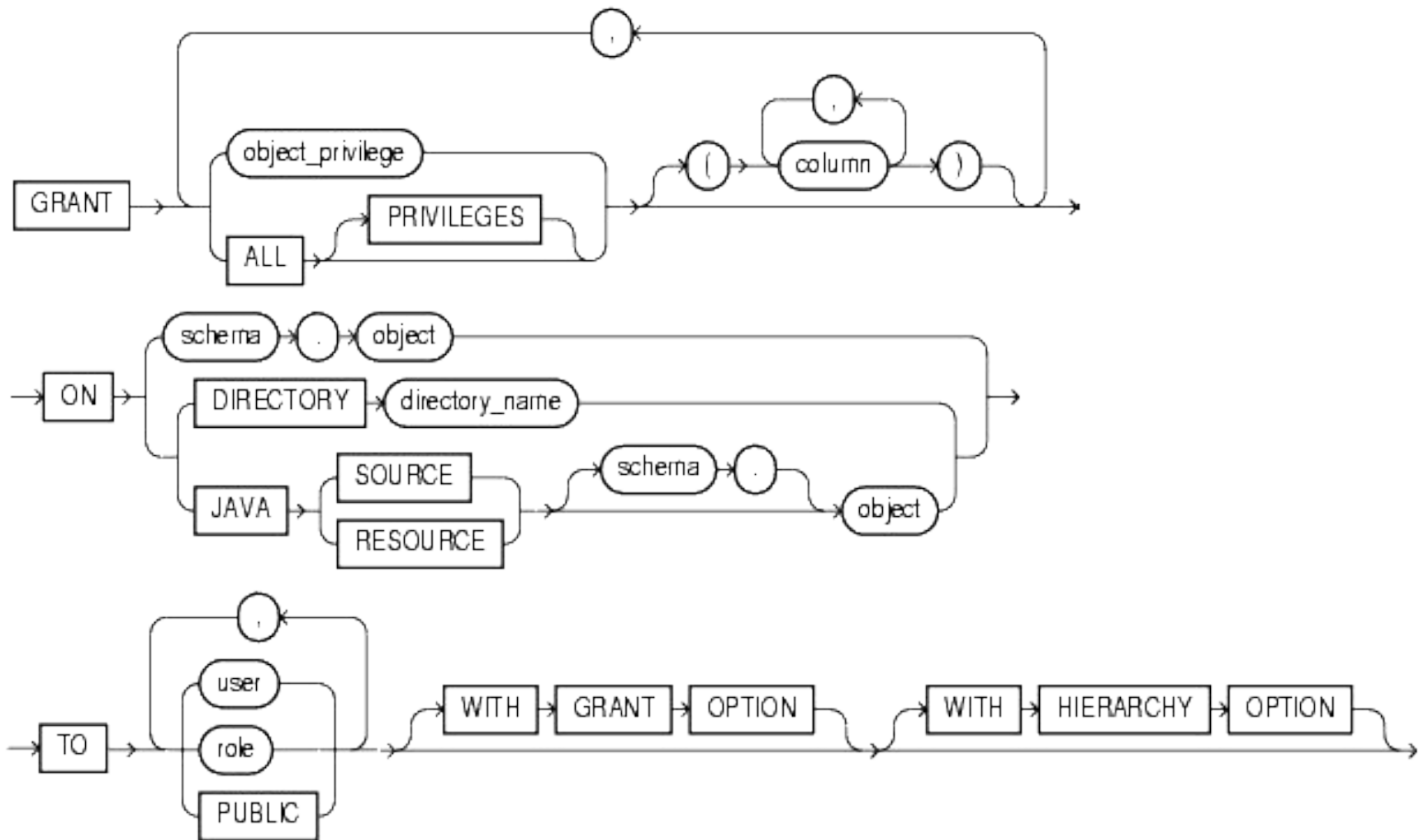
# У каждого объекта БД имеется свой набор привилегий

Привилегии на объект	TABLE	VIEW	SEQUENCE	PROCEDURE
ALTER	+		+	
INSERT	+	+		
UPDATE	+	+		
DELETE	+	+		
SELECT	+	+	+	
REFERENCES	+			
INDEX	+			
EXECUTE				+

# Объектные привилегии

- Объектные привилегии зависят (меняются) от объекта БД.
- Владелец объекта имеет ВСЕ привилегии на этот объект.
- Владелец объекта может предоставлять конкретные привилегии на объект другим пользователям.
- Выдача объектных привилегий выполняется командой GRANT.

# Синтаксис команды GRANT для объектных привилегий



# Синтаксис команды GRANT

**GRANT** объект\_привил [колонки]

**ON** объект

**TO** [пользователь | роль | PUBLIC]

**[WITH GRANT OPTION]**

Пример:

**GRANT select ON emp TO petr;**

**GRANT insert, update(sal) ON emp TO ivan;**



# Указания по назначению объектных привилегий

- Вы можете предоставлять привилегии на объект другим пользователям в случае, если:
  - **этот объект находится в вашей собственной схеме**
  - вы получили привилегии на него с ключевым словом **WITH GRANT OPTION**.
- Владелец объекта может предоставить любую объектную привилегию на него любому другому пользователю или роли в БД.
- **Владелец объекта приобретает все объектные привилегии на этот объект автоматически.**

# Назначение объектных привилегий

Объектные привилегии на таблицу в целом:

- Все привилегии:

```
GRANT all ON emp TO ivan;
```

- Конкретные привилегии:

```
GRANT select, insert, update ON emp TO ivan;
```

- Объектные привилегии на столбцы таблицы:

```
GRANT insert(ename, sal), update(ename, sal)  
ON emp TO ivan;
```

# Ключевые слова WITH GRANT OPTION и PUBLIC

- Пользователь, получивший привилегию с ключевым словом **WITH GRANT OPTION**, может каскадно передавать ее другим пользователям или ролям.
- **Ключевое слово PUBLIC**  
Владелец таблицы может разрешить доступ всем пользователям, зарегистрированным в базе данных, с помощью ключевого слова **PUBLIC** ("общедоступный").

# Примеры

- Предоставление пользователю права на передачу привилегий

```
SQL>GRANT select, insert ON emp  
2 TO petr WITH GRANT OPTION;
```

- Предоставление разрешения всем пользователям системы на выборку данных из таблицы EMP, принадлежащей пользователю IVAN.

```
SQL>GRANT select ON ivan.emp TO PUBLIC;
```

# Проверка предоставленных привилегий

- Если пользователь попытается выполнить неразрешенную операцию (например, удалить строку из таблицы, на которую у него нет привилегии DELETE), сервер Oracle автоматически отследит эту ситуацию и не допустит выполнения операции.
- Если сервер Oracle выдает сообщение об ошибке "таблица или представление не существует" (***table or view does not exist***), причина может быть в следующем:
  - Ссылка на несуществующую таблицу или представление
  - Попытка выполнить операцию с таблицей или представлением, на которые у пользователя нет соответствующих привилегий.

# Обзоры словаря БД

Пользователь может проверить свои привилегии по словарю базы данных.

Обзоры словаря БД	Описание
<b>USER_TAB_PRIVS_MADE</b>	Объектные привилегии, предоставленные пользователем на его объекты
<b>USER_TAB_PRIVS_RECD</b>	Объектные привилегии, предоставленные пользователю
<b>USER_COL_PRIVS_MADE</b>	Привилегии, предоставленные пользователем на столбцы его объектов
<b>USER_COL_PRIVS_RECD</b>	Привилегии на столбцы чужих объектов, предоставленные пользователю

# Отмена объектных привилегий

- Для отмены объектных привилегий, предоставленных другим пользователям, используется команда REVOKE.
- Одновременно отменяются привилегии, предоставленные другим пользователям, с помощью опции WITH GRANT OPTION.

REVOKE {привлегия [,привилегия] | ALL}

ON объект

FROM пользователь | роль | PUBLIC

[CASCADE CONSTRAINTS]

# Пример

Отмена объектных привилегий SELECT, INSERT, предоставленных пользователю IVAN на таблицу EMP:

```
SQL>REVOKE select, insert
```

```
2 ON emp
```

```
3 FROM ivan;
```

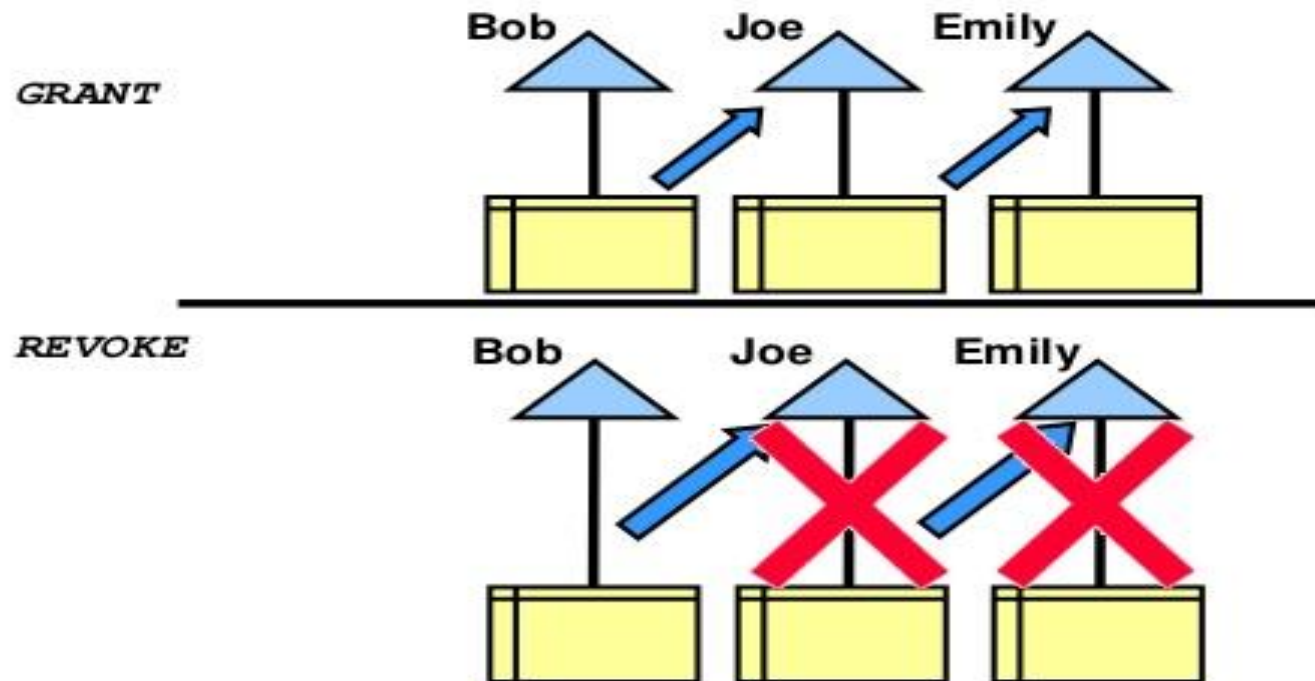
```
Revoke succeeded.
```



# Отмена объектных привилегий, выданных с GRANT OPTION

YUNHE

## Revoking Object Privileges with *GRANT OPTION*



# ИТОГИ

- Без специального разрешения **пользователи имеют доступ только к своим собственным объектам.**
- Для доступа к объектам «чужих» схем **пользователь должен получить объектные привилегии.**
- Владелец объекта может предоставить любую объектную привилегию на него другому пользователю или роли в БД.